Claims:

Sub a1

1. A method for time stamping a document comprising:

a. receiving a time stamp request at an outside agency at a first time, said time stamp request including identifying data associated with said document;

b. creating at said outside agency a time stamp receipt based on said identifying data and a time indication; and

c. generating at said outside agency a message authentication code based on said time stamp receipt and a secret key;

d. transmitting said time stamp receipt and said message authentication code to a designated party;

e. receiving a certification request at said outside agency at a second time, said certification request including said time stamp receipt and said message authentication code;

f. validating said message authentication code at said outside agency using said secret key; and

g. certifying said time stamp receipt at said outside agency using a cryptographic signature scheme if said message authentication code is valid.

2. The time stamping method of claim 1 wherein said identifying data comprises a digital representation of at least a portion of said document.

3. The time stamping method of claim 2 wherein said identifying data comprises a digital sequence derived by application of a deterministic function to at least a portion of said document.

4. The time stamping method of claim 3 wherein said digital sequence is a hash value derived by application of a one-way hashing function to at least a portion of said document.

5. The time stamping method of claim 1 wherein said time stamp receipt includes a copy of at least a portion of said identifying data concatenated with said time indication.

6. The time stamping method of claim 5 wherein said time stamp receipt includes a digital sequence derived from said identifying data concatenated with said time indication.

7. The time stamping method of claim 1 wherein said time stamp request further includes an identification number associated with the requestor.

8. The time stamping method of claim 1 wherein said message authentication code comprises a digital sequence generated by application of a deterministic function to said time stamp receipt and said secret key concatenated together.

9. The time stamping method of claim 6 wherein the step of validating said message authentication code includes recomputing said message authentication code at said outside agency using said received time stamp receipt and said secret key and comparing the recomputed message authentication code to said received message authentication code.

10. The time stamping method of claim 1 wherein the certifying step includes signing said message authentication code using a private signature key controlled by said outside agency.

11. The time stamping method of claim 1 wherein the certifying step includes signing said time stamp receipt using a private signature key controlled by said outside agency.

12. The time stamping method of claim 1 further including the step of storing said secret key in a database at said outside agency.

13. The time stamping method of claim 1 wherein each time stamp receipt includes a sequential record number that is used at said outside agency to look up said secret key in said database.

14. The time stamping method of claim 1 further including the step of transmitting said certified time stamp receipt to said requestor.

15. A method for time stamping a document comprising:

a. receiving a time stamp request at an outside agency at a first time, said time stamp request including identifying data associated with said document;

b. creating at said outside agency a time stamp receipt based on said identifying data and a time indication; and

c. generating at said outside agency a message authentication code based on said time stamp receipt and a secret key;

d. encrypting the secret key with a second secret key to generate a key message;

e. generating a second message authentication code based on said first message authentication code and said first secret key using said second secret key;

f. transmitting said time stamp receipt, said first message authentication code, said second message authentication code, and said encrypted key message to said requestor;

g. receiving at said outside agency at a second time a certification request, said certification request including said time stamp receipt, said first message authentication code, said second message authentication code, and said encrypted key message;

f. decrypting at said outside agency said encrypted key message to recover said first secret key;

g. validating said second message authentication code at said outside agency using said second secret key;

h. validating said first message authentication code at said outside agency using said first secret key if said second message authentication code is valid; and

i. certifying said first message authentication code at said outside agency using a cryptographic signature scheme if said first message authentication code is valid.

16. The time stamping method of claim 15 wherein said identifying data comprises a digital representation of at least a portion of said document.

17. The time stamping method of claim 16 wherein said identifying data comprises a digital sequence derived by application of a deterministic function to at least a portion of said document.

18. The time stamping method of claim 17 wherein said digital sequence is a hash value derived by application of a one-way hashing function to at least a portion of said document.

19. The time stamping method of claim 17 wherein said time stamp receipt includes a copy of at least a portion of said identifying data concatenated with said time indication.

20. The time stamping method of claim 19 wherein said time stamp receipt includes a digital sequence derived from said identifying data concatenated with said time indication.

21. The time stamping method of claim 15 wherein said time stamp request further includes an identification number associated with the requestor.

22. The time stamping method of claim 15 wherein said first message authentication code comprises a numeric representation generated by application of a deterministic function to said time stamp receipt and said secret key concatenated together.

23. The time stamping method of claim 22 wherein said second message authentication code comprises a numeric representation generated by application of a deterministic function to said first message authentication code concatenated with said first and second secret keys.

24. The time stamping method of claim 23 wherein the step of validating said second message authentication code includes recomputing said second message authentication code at said outside agency using said first message authentication code received as part of said certification request and said secret key and comparing the recomputed second message authentication code to said received second message authentication code.

25. The time stamping method of claim 24 wherein the step of validating said first message authentication code includes recomputing said first message authentication code at said outside agency using said time stamp receipt received as part of said certification request and said first secret key and comparing the recomputed first message authentication code to said received first message authentication code.

26. The time stamping method of claim 15 wherein the step of certifying said time stamp receipt includes signing said first message authentication code using a private signature key controlled by said outside agency.

27. The time stamping method of claim 15 wherein the step of certifying said time stamp receipt includes signing said time stamp receipt using a private signature key controlled by said outside agency.

28. The time stamping method of claim 15 further including the step of transmitting said certified time stamp receipt to said requestor.

29. A method for time stamping a document comprising:

a. receiving a time stamp request at an outside agency at a first time, said time stamp request including identifying data associated with said document;

b. creating at said outside agency a time stamp receipt based on said identifying data and a time indication; and

c. generating at said outside agency a message authentication code based on said time stamp receipt and a secret key; and

d. transmitting said time stamp receipt and said message authentication code to said requestor.

30. The time stamping method of claim 29 wherein said identifying data comprises a digital representation of at least a portion of said document.

31. The time stamping method of claim 30 wherein said identifying data comprises a digital sequence derived by application of a deterministic function to at least a portion of said document.

32. The time stamping method of claim 31 wherein said digital sequence is a hash value derived by application of a one-way hashing function to at least a portion of said document.

33. The time stamping method of claim 29 wherein said time stamp receipt includes a copy of at least a portion of said identifying data concatenated with said time indication.

34. The time stamping method of claim 23 wherein said time stamp receipt includes a digital sequence derived from said identifying data concatenated with said time indication.

35. The time stamping method of claim 29 wherein said time stamp request further includes an identification number associated with the requestor.

36. The time stamping method of claim 29 wherein said message authentication code comprises a numeric representation generated by application of a deterministic function to said time stamp receipt and said secret key concatenated together.

37. The time stamping method of claim 29 further including generating a second message authentication code based on said first message authentication code and a second secret key.

38. The time stamping method of claim 37 further including transmitting said second message authentication codes to said requestor.

39. The time stamping method of claim 37 further including the step of encrypting the first secret key to generate an encrypted key.

40. The time stamping method of claim 39 further including transmitting said encrypted key to said requestor.

41. A method for time stamping documents comprising:

a. receiving at an outside agency a certification request, said certification request including a time stamp receipt and a message authentication code generated on said time stamp receipt;

b. validating said message authentication code at said outside agency using a secret key;

c. certifying said time stamp receipt if said message authentication code is valid using a cryptographic signature scheme.

42. The time stamping method of claim 41 wherein the step of certifying said time stamp receipt includes signing said message authentication code at said outside agency using a cryptographic signature scheme.

43. The time stamping method of claim 41 wherein the step of certifying said time stamp record includes signing said time stamp receipt at said outside agency using a cryptographic signature scheme.

44. The time stamping method of claim 41 further including the step of transmitting said certified time stamp receipt to said requestor.